

EDOK - Application for Search Warrant (Revised 5/13)

United States District Court

EASTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF:
One (1) Samsung SM-S767VL Galaxy J7 Crown
touch screen phone, IMEI: 356823094531154

Case No. 21-MJ-281-KEW

APPLICATION FOR SEARCH WARRANT

I, Jenny Shelton, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the EASTERN District of OKLAHOMA (*identify the person or describe property to be searched and give its location*):

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal (*identify the person or describe the property to be seized*):

SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Sections 1519 and 2252(a)(4), (b)(2), and the application is based on these facts:

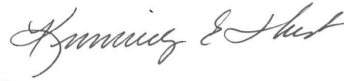
- ☒ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: June 16, 2021

City and state: Muskogee, Oklahoma


JENNY SHELTON
SPECIAL AGENT, FBI



Judge's signature

UNITED STATES MAGISTRATE JUDGE
Printed name and title



**UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF OKLAHOMA**

**IN THE MATTER OF THE SEARCH OF:
One (1) Samsung SM-S767VL Galaxy J7
Crown touch screen phone, bearing IMEI:
356823094531154**

Case No.

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Jenny Shelton, a Special Agent with the Federal Bureau of Investigation (FBI),
being duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a search warrant authorizing the examination of property—two cellphones—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been employed as a Special Agent with the FBI since May 2019. I am currently permanently assigned to the Boston Division of the FBI and am temporarily assigned to the Oklahoma City Division, Muskogee Resident Agency. My duties include, among other things, the investigation of violent crimes and sexually based offenses occurring within Indian Country. While employed with the FBI, I have investigated and participated in investigations involving federal criminal violations related to gang activities, drug trafficking, firearms offenses, white collar crimes, and other crimes.

3. As a Special Agent, I am authorized to investigate violations of the criminal laws of the United States, to enforce those laws, and to request and execute search warrants and arrest warrants issued under the authority of the United States.

4. This Affidavit contains information necessary to support probable cause for this application. It is not intended to include every fact or detail observed by me or known by law enforcement. Additionally, unless otherwise indicated, wherever in this Affidavit I assert that an individual made a statement, that statement is described in substance herein and is not intended to be a verbatim recitation of such statement. Furthermore, unless otherwise indicated, all statements contained in this Affidavit are summaries in substance and in part. The following is true to the best of my knowledge and belief.

5. The statements set forth in this Affidavit are based in part on: my personal knowledge and investigation; my training and experience as a Special Agent with the FBI; information obtained from other individuals, including other law enforcement officers and agencies; and my review of documents, interview reports, witness testimony, and other materials related to this investigation.

6. I submit this Affidavit in support of applications for search warrants to search a Samsung SM-S767VL(GP) touch screen phone, bearing IMEI: 357092101625271 and belonging to PHILLIP RYAN STANLEY that was initially seized pursuant to an October 11, 2019, search warrant executed and issued by the District Court of Adair County; and to search a Samsung SM-S767VL Galaxy J7 Crown touch screen phone, bearing IMEI: 356823094531154 and belonging to PHILLIP RYAN STANLEY that was initially seized pursuant to a September 18, 2019, search warrant executed and issued by the District Court of Adair County. The FBI took custody of these devices on June 11, 2021.

7. As detailed below, I have probable cause to believe that evidence (including among other things messages, photos, and videos) of violations of Title 18, United States Code, Sections 1151, 1153, and 2243(a) (which, together, comprise Sexual Abuse of a

Minor in Indian Country) may be located and found within the devices listed above and described in Attachment A incorporated with this Affidavit. The applied-for warrant would authorize the forensic examination of the devices for the purpose of identifying electronically stored data particularly described in Attachment B.

STATUTORY AUTHORITY

8. I know from my previous training and experience that pursuant to Title 18, United States Code, Section 2243(a) it is unlawful for any person to knowingly engage in a sexual act with another person who (a) has attained the age of 12 years, (b) has not attained the age of 16 years, and (c) is at least four years younger than the person so engaging.

PROBABLE CAUSE

9. **Criminal Actor:** The individual who potentially engaged in criminal activity relevant to this search warrant is PHILLIP RYAN STANLEY, date of birth XX/XX/1991. For purposes of federal jurisdiction, STANLEY is an Indian and is an enrolled member of the Cherokee Nation. A federal grand jury has charged STANLEY with twelve counts of Sexual Abuse of a Minor in Indian Country for the acts detailed herein. *See United States v. Stanley*, No. 21-CR-073 (E.D. Okla.).

10. **Victim:** K.M., date of birth XX/XX/2003. K.M. is the stepdaughter of PHILLIP STANLEY.

11. **Jurisdiction:** The facts and circumstances alleged in this Affidavit occurred within the Eastern District of Oklahoma, and the item to be searched is located in the Eastern District of Oklahoma. In addition, the sexual acts described below occurred within the reservation boundaries of the Cherokee Nation and therefore, within Indian Country.

12. **STANLEY engages in sexual acts with K.M.:** K.M. was interviewed by law enforcement and DHS, and provided sworn testimony, about her relationship with STANLEY.

13. In 2017, STANLEY was released from prison and moved back to Oklahoma. Shortly after, STANLEY moved into a home in Watts, OK, Adair County with his wife, his two children, and his two stepchildren. One of STANLEY's stepchildren was K.M., a fourteen-year-old girl. K.M. had known STANLEY since she was eight but noticed a change in his behavior when they moved into the home. K.M. recalled STANLEY started constantly wrestling with her, telling her he loved her, hugging her, and calling her beautiful, sexy, and "hon." Soon, he was messing with her more and touching her more. Eventually, K.M. thought she was in love with him, even though she knew that STANLEY had multiple girlfriends, not to mention her mother, STANLEY's wife.

14. During her testimony, she stated that in the summer of 2018, prior to K.M.'s fifteenth birthday on September 3, STANLEY entered her bedroom early in the morning, after her mom left for work. He laid down on her bed and touched her breasts, butt, and vagina with his hands.

15. A "few days" later, the same thing happened.

16. Roughly a week later, when K.M. was still fourteen, STANLEY again came to her room, but this time STANLEY removed K.M.'s pants and underwear, touched her breasts, butt, and vagina, and engaged in vaginal intercourse with K.M.

17. From that point on, K.M. and STANLEY had sex "[p]robably once a week," usually in her bedroom, but sometimes in her mother's room or STANLEY's truck. Each encounter occurred in Adair County, and STANLEY always used a condom.

18. STANLEY continued having sex with K.M. on a weekly basis until K.M. moved in with her aunt in the middle of August 2019, when K.M. was still fifteen years old.

19. **STANLEY used cellphones to communicate with K.M., and K.M. testifies that evidence of her relationship with STANLEY would be located on cellphones:** After their relationship came to light and Oklahoma Department of Human Services (DHS) and law enforcement were investigating STANLEY, he tried all avenues to contact K.M. He sent messages to K.M. and her friends, contacted her mother and aunt to see if they would allow him to speak with her, and went to her school. K.M. was in “great fear” of STANLEY.

20. During the course of the investigation, STANLEY sent investigators a video he took during an altercation with his wife, which showed his wife stating STANLEY is “fucking” K.M. and “that is why he goes into her bedroom at night.”

21. In her sworn testimony, when asked if she had information to verify what she said happened with STANLEY, K.M. stated she thought there was information on cellphones and that the cellphone she had at the time had been given to law enforcement. K.M. also stated she had sent a Snapchat message to an adult friend of STANLEY’s named “Stetson” talking about STANLEY going to prison.

22. Linda White, K.M.’s aunt, was interviewed by DHS. She indicated to the interviewer that K.M. had told her that there were messages of a sexual nature between her and STANLEY on her cellphone.

23. Linda White also told DHS that during a supervised visit involving STANLEY and his minor children, his minor child J.S. was playing with STANLEY’s phone. While J.S. had the phone, K.M.’s Snapchat picture appeared in a notification on

STANLEY's phone. J.S. stated K.M. sent STANLEY multiple Snapchats while J.S. had STANLEY's cellphone.

24. Screenshots of the Snapchat exchange showed K.M. sending STANLEY a bitmoji (*i.e.*, a software-generated personal avatar) picture of K.M. and STANLEY's respective bitmojis, with K.M.'s bitmoji holding three balloons (a heart, a heart-eyed, and a kissing face balloon). STANLEY's profile replies to the message stating "I love you."

25. Jennifer White, K.M.'s mother, was interviewed by DHS. She indicated to the interviewer that she had observed Snapchat notices and text messages on K.M.'s phone from STANLEY.

26. STANLEY told a DHS interviewer that he communicated with K.M. regularly by phone, including by Snapchat, Facebook, and text message. STANLEY used Snapchat to communicate with K.M. even though he was not allowed to by the terms of his probation.

27. On October 11, 2019, when law enforcement executed an arrest warrant on STANLEY, STANLEY was utilizing a cellular telephone. Law enforcement seized that phone pursuant to a warrant and has maintained custody of that cell phone since that time. Law enforcement had previously seized STANLEY's cellular telephone pursuant to the September 18, 2019, warrant and maintained custody of that cellphone as well. (See paragraph 6 for additional detail.)

28. After STANLEY was arrested on federal charges, the FBI took custody of the Samsung SM-S767VL(GP) touch screen phone bearing IMEI: 357092101625271 and the Samsung SM-S767VL Galaxy J7 Crown touch screen phone bearing IMEI: 356823094531154 on June 11, 2021, and entered them into evidence.

29. While the FBI might already have all necessary authority to examine these devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the devices will comply with the Fourth Amendment and other applicable laws.

30. In my training and experience, and based on my discussions with other law enforcement officers, and their training and experience, I know that the devices described in Attachment A have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of law enforcement in September and October 2019.

31. In addition, based on my training and experience, use of multiple forms of social media are common. In other words, the use of Snapchat and Facebook does not exclude the use of other forms of social media, such as Twitter, Instagram, and others. Therefore, communication from STANLEY regarding K.M. is likely present on those platforms as well.

32. **Electronic Storage and Forensic Analysis:** Based on my knowledge, training, and experience, and the knowledge, training and experience of other law enforcement officers with whom I have had discussions, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

33. There is probable cause to believe that communications, images, videos, and other forms of records and information that were once stored on the devices referenced herein may still be stored there, for at least the following reasons:

34. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

35. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer (and from there to an external hard drive, CD-ROM disk, or other storage device) by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These phones themselves and the memory cards are often large enough to store thousands of high-resolution photographs or videos.

36. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Communications, images, videos, and other records and information, therefore, therefore be easily, inexpensively and even anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

37. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes

referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence regarding sexual contact with a child can be found on the user’s computer, smartphone or external media in most cases.

38. As is the case with most digital technology, communications by way of computer and smartphone can be saved or stored on the device used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

39. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

40. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

41. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

42. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

43. **Forensic Evidence:** As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices discussed above and in Attachment A were used, the purpose of their use, who used the devices, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

44. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as

online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

45. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

46. A person with appropriate familiarity with how electronic devices work may, after examining this forensic evidence in its proper context, be able to draw conclusions as to how the devices were used, the purpose of use, who used them, and when.

47. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

48. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

49. In addition, I know that when an individual uses an electronic device to delete, destroy, transfer, or save electronic files, the electronic device used will generally serve both as an instrumentality for committing the crime, and also as a storage medium

for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

50. **Nature of examination:** Based on the foregoing, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire mediums, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

51. **Manner of execution:** Because this warrant seeks only permission to examine devices already in law enforcement's possession, execution of this warrant does not involve the physical intrusion onto a premises. Thus, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

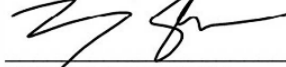
CONCLUSION

52. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the devices described in Attachment A to seek the items described in Attachment B.

53. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab; digital evidence will also undergo a similar process. For this reason, unless

otherwise ordered by the Court, the “return” will not include evidence examined by a forensic analyst.

Respectfully submitted,

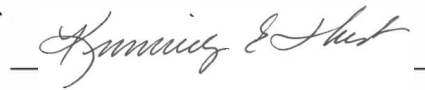


JENNY SHELTON

Special Agent

Federal Bureau of Investigation

Subscribed and sworn to before me this 16th day of June, 2021.



United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

All items of digital technology seized pursuant to a September 18, 2019, search warrant executed and issued by the District Court of Adair County. Said items were taken into the custody of the Federal Bureau of Investigation (FBI) on June 11, 2021, and remain in the custody of the FBI in the Eastern District of Oklahoma at this time. Specifically, those items of digital technology are:

- (a) Samsung SM-S767VL Galaxy J7 Crown touch screen phone, bearing IMEI:
356823094531154

This warrant authorizes the forensic examination of the devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

- A. All records on the devices described in Attachment A that relate to violations of 18 U.S.C. § 2243(a) and involve PHILIP RYAN STANLEY, including:
 - a. All stored electronic and wire communications and information in memory on the mobile device, in any form kept, including, email, chat logs, instant messaging, text messages, other communications or correspondence, contact lists, travel records or other evidence indicating the geographic location of the cellular device at times relevant to the investigation, information related to the identity of victims, photographs/images (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), videos (including, but not limited to, stories, text-based files, motion pictures, films, and other recordings), and any other content or records on the phone; and
 - b. All files, data, metadata, and data of any type relating to saving, deleting, transferring, or otherwise altering records located on the devices.
- B. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
- C. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;
- D. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;
- E. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;
- F. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and
- G. Records or other items which evidence ownership or use of computer equipment or any of the devices described in this attachment, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;

- H. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.
- I. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Federal Bureau of Investigation may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.